REMARKS

Claims 8, 35-41, 50-57, and 64-72 are pending in this application. Claims 8, 38, 50, 54, 64, 68, and 72 are amended herein. Support for the amendments to claims 4, 38, 50, 54, 64, 68, and 72 may be found in the claims as originally filed, and in the specification at, inter alia, page 20, line 24. Claims 4, 9, 32, 33, and 34 are canceled herein without prejudice or disclaimer. Reconsideration is requested based on the foregoing amendment and the following remarks.

Interview Summary

The Applicants submit the following summary of the telephone interview that took place October 2, 2006 between the undersigned representative of the Applicants and the Examiner.

Telephone Conference:

The Applicants thank the Examiner for the many courtesies extended to the undersigned representative of the Applicants during the telephone interview that took place October 2, 2006.

Among the issues discussed during that interview was objection to the drawings at page 3, in section 5 of the Office Action, in which the output of the Sbox is stated to correspond to $S_j[Y]$. This characterization of the output of the Sbox is believed to be incorrect. If further discussion would help resolve this issue, the courtesy of a telephone call to the undersigned is requested.

Objections to the Abstract of the Disclosure:

The Abstract of the Disclosure has been objected to for including the term "means." The Abstract has consequently been re-written on a separate sheet without using the term "means." No new matter has been added. Withdrawal of the objection is earnestly solicited.

Objections to the Specification:

The Specification has been objected to for not defining s[x], s[x XOR ci,j] XOR di,j, and $S_j[x]$. To the contrary, these terms are believed to be described at, inter alia page 26, lines 7-29. The specification is believed to provide proper antecedent basis for the claimed subject matter. If further discussion would help resolve this issue, the courtesy of a telephone call to the undersigned is requested. Otherwise, withdrawal of the objection is earnestly solicited.

At this time, three representations are used to represent Sboxes for consistency in the

amended claims and the specification, as follows:

Representation 1:

S[x]: represents Sbox in the conventional Rijndael Process.

Representation 2:

$S_{i,j,h}[x] = S[x \text{ XOR } c_{i,j,h}] \text{ XOR } d_{i,j,h}$ or

$S[x \oplus c_{i,j,h}] \oplus d_{i,j,h}$ (as shown in Fig. 28)

where i represents i-th round (as shown in Fig. 27) (i=0,1,..,N-1),
j represents j-th Sbox in the conventional Rijndael process (j =0,1,2,...,15),
h represents a random number (h=0,1, ... q-1), and $c_{i,j,h}$, $d_{i,j,h}$ are constants.
Different sets of Sbox tables $S_{i,j,h}[x]$ are used in different i-th rounds.

Representation 3:

$S_{j,h}[x] = S[x \text{ XOR } c_{h,j}] \text{ XOR } d_{h,j}$ or

$S[x \oplus c_{h,j}] \oplus d_{h,j}$ (as shown in Fig. 28)

where the suffix i in Representation 2 is omitted because the same set of Sbox
tables $S_{i,j,h}[x]$ are used in different i-th rounds, and $c_{h,j}$, $d_{h,j}$ are constants (where
the positions of h and j are switched in Representation 2).

Representations 1 and 3, <u>inter alia</u>, are used in the claims. In the amended claims, the fixed Sbox table and the fixed mask values are defined as different sets of elements, and "FMin" has been amended to --$Fmin_h$-- for consistency with the specification. Finally, "$S_{i,h}$" has been replaced with "$S_{j,h}$" in the paragraph at page 41, lines 1-15.

Objections to the Drawings:

The drawings were objected to for defining an output of an Sbox as Y. To the contrary, the equation $S_{i,j,h}(x) = S (x \oplus a_{i,j,h}) \oplus b_{i,j,h}$ in Fig. 28 represents a conventional Rijndael process, as discussed above. If further discussion would help resolve this issue, the courtesy of a telephone call to the undersigned is requested. Withdrawal of the objections to the drawings is earnestly solicited.

Objections to the Claims:

Claims 8 and 37 were objected to for various informalities. Claims 8 and 37 were amended in substantial accord with the Examiner's suggestions. The Examiner's suggestions are appreciated. Withdrawal of the objection is earnestly solicited.

Claim Rejections - 35 U.S.C. § 112:

Claims 8, 35-41, 50-57, and 64-72 were rejected under 35 U.S.C. § 112, second paragraph, as indefinite. Claims 8, 38, 50, 54, 64, 68, and 72 were amended to make them more definite. Claim 8, for example, now recites:

"q sets of fixed S-box tables," rather than "q sets of fixed values;"

"q sets of fixed mask values $FM_{i,h}$" rather than "q sets of fixed values;" and

"$S_{j,h}[x] = S[x\ XOR\ c_{i,j}]\ XOR\ d_{h,j}$," rather than "$S_j[x\ XOR\ c_{i,j}]\ XOR\ d_{i,j}$."

The Office Action asserts in section 15 that claims 8, 35-41, 50-57, and 64-72 contain contradictory definitions of the transform means. The first and second transform means in claims 8, 35-41, 50-57, and 64-72, to the contrary, can be defined as:

$L1i(x) = x$ and $L2i(x) = MixedColumn(Shift(x))$

or

$L2i(x) = Shift(x)$,

where x, $Shift(x)$ and $MixedColumn(Shift(x))$ are linear transforms.

Claims 8, 35-41, 50-57, and 64-72 are thus believed to be definite within the meaning of 35 U.S.C. § 112, second paragraph. Withdrawal of the rejection is earnestly solicited.

Claim Rejections - 35 U.S.C. § 102:

Claims 8, 35-41, 50-57, and 64-72 were rejected under 35 U.S.C. § 102(b) as anticipated by European Patent Application No. EP 0 981 223 to Kawamura et al. (hereinafter "Kawamura"). The rejection is traversed to the extent it might apply to the claims as amended. Reconsideration of the rejection is requested.

The following FIGS. A and B illustrate the distinction of the present invention over the Kawamura et al. (EP 0981223 A2).

FIG. A - Application of KAWAMURA et al. (EP 0981223) of the Rijndael process is shown on the following page:

14
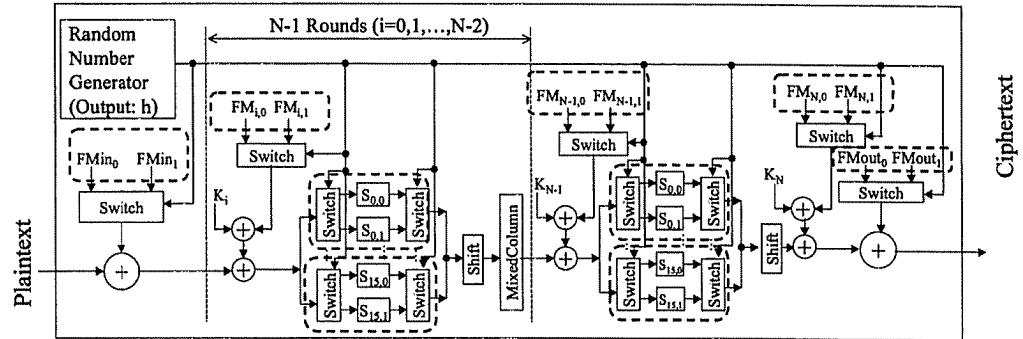
Where, q=2 and $FM_{i,0} \oplus FM_{i,1} = (1111.....1111)_2$ holds for all i=0,...,N+1, $S_{j,h}[x] = S[x \oplus c_{h,j}] \oplus d_{h,j}$

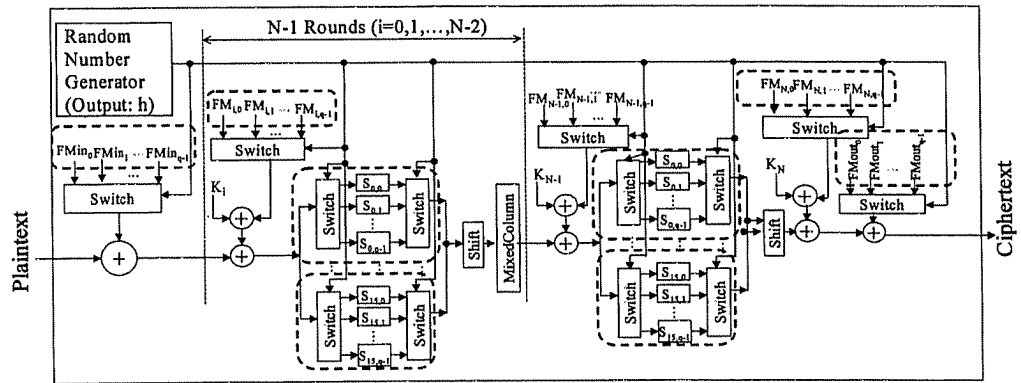And, $WC_j = c_{0,j} \oplus c_{1,j} = (11111111)_2$, $WD_j = (d_{0,j} \oplus d_{1,j}) = (11111111)_2$ for all j=0,...,15.

$FM_{i,h}$ is defined by equation (11) in the description of our invention,

and C_h, D_h are defined by equation (12) in the description of our invention.

Note: Every fixed mask values ($FMin_h$, $FM_{i,h}$, $FMout_h$) and fixed Sbox tables ($S_{j,h}$) are chosen by **1 out of 2** in accordance with a random number h (h=0,1).

FIG B – The application of the present invention of the Rijndael process (FIG.23 with FIG.29) is shown on the following page:

Where, q=2 and $FM_{i,0} \oplus FM_{i,1} = (1111.....1111)_2$ holds for all i=0,...,N+1

Hence, $WC_j = c_{0,j} \oplus c_{1,j} = (11111111)_2$, $WD_j = (d_{0,j} \oplus d_{1,j}) = (11111111)_2$ for all j=0,...,15.

$FM_{i,h}$ is defined by equation (11) in the description of our invention,

and C_h, D_h are defined by equation (12) in the description of our invention.

Note: Every fixed mask values ($FMin_h$, $FM_{i,h}$, $FMout_h$) and fixed Sbox tables ($S_{j,h}$) are chosen by **1 out of q (q≥3)** in accordance with a random number h (h=0,1,...q-1).

As shown in FIG. A above, in the application of Kawamura of the Rijndael process, it selects one out of two in response to the random number. In contrast, as shown FIG. B above, in the application of the present invention of the Rijndael process, it selects one out of one, which is q, which is not smaller than three (q ≥ 3). This difference leads to the distinction and advantage of the present invention in terms of its security over Kawamura.

In FIG. A above, in the application of Kawamura of the Rijndael process, one of the fixed mask values is a complement of the other, and one of the fixed Sbox tables is a complement of the other. For example, if the one fixed mask value is $FM_{0,0} = (01011100)_2$, then the other fixed mask value is $FM_{0,1} = (01011100)_2$. Similarly, one of the constants $c_{h,j}$ for the fixed Sbox table is complement of the other, and one of the constants $d_{h,j}$ for the fixed Sbox table is complement of the other. See Kawamura, paragraphs 0009-0013, FIGS. 4, 5A, 5B, 11, 12, 14 and 15.

This complementary relation can be expressed for $c_{h,j}$ and $d_{h,j}$ as follows:

$$c_{0,j} \oplus c_{1,j} = (11111111)_2 \, , \, d_{0,j} \oplus d_{1,j} = (11111111)_2 \quad ...(E1)$$

which corresponds to Equations (15) and (16) for q=2 in page 33 in the specification of the subject application.

Selecting one of the two fixed mask values and one of two fixed Sbox tables is vulnerable to the DPA as shown in Table 2 in "Adjacent Bit Model" in the specification of the subject application. The amount of computation for key analysis of a 128-bit secret key in this case is only 2^{23}.

In contrast, in FIG. B above, in the application of the present invention of the Rijndael process, fixed mask values and fixed Sbox tables need not satisfy the complementary relations. However, $c_{h,j}$ and $d_{h,j}$ which determine the input and output of the fixed Sbox tables are required to satisfy Equations (Equations (15) and (16) in page 33 in the specification) as follows:

$$(c_{0,j} \text{ XOR } c_{1,j}) \vee (c_{1,j} \text{ XOR } c_{2,j}) \vee ... \vee (c_{q-2,j} \text{ XOR } c_{q-1,j}) = (111..11)_2$$

$$(d_{0,j} \text{ XOR } d_{1,j}) \lor (d_{1,j} \text{ XOR } d_{2,j}) \lor ... \lor (d_{q-2,j} \text{ XOR } d_{q-1,j}) = (111..11)_2$$

$$...(E2)$$

Equations E2 are equivalent for q=2. However, for q≥3, the security is very high, even in the Adjacent Bit Mode. The security for q≥3 can be evaluated according to the specification, page 38, line 8 (last line) to page 39, line 6 (1. ...) for $d_{h,j}$ (see Equation (16) in page 33), and lines 22-29 (4. ...) for $c_{h,j}$ (see Equation (15) in page 33). The amount of computation for key analysis of a 128-bit secret key in this case is as high as 2^{128}.

Kawamura allows three or more mask values FMi_{nh}, $FM_{0,h}$, ... $FM_{N,h}$, $FMout_h$ (see FIG. A above), each mask value is selected from two mask values according to a random number, but not from three or more mask values as defined in the present invention. This is described in Kawamura in paragraph 9, "means for randomly selecting one pattern of each pairs". In contrast, each mask value is selected from three or more mask values according to a random number in the present invention (see FIG. B above).

The Office Action asserts in section 20 that the Hamming weights indicate the subject matters of claims 8, 50, 64 72. This is statement is submitted to be incorrect.

In Kawamura, one value is selected from the two values:

$c_{0,j}=(1\ 0\ 1\ 0\ 1\ 1\ 0\ 0)_2$

$c_{1,j}=(0\ 1\ 0\ 1\ 0\ 0\ 1\ 1)_2$

where 1's appear at probability of 1/2 vertically and horizontally. Hence, the average Hamming weight is 1/2.

In the present invention, one value is selected from three or more values such as:

$c_{0,j}=(1\ 0\ 1\ 1\ 1\ 0\ 1\ 1)_2$

$c_{1,j}=(0\ 1\ 1\ 1\ 0\ 0\ 1\ 0)_2$

$c_{2,j}=(1\ 1\ 0\ 1\ 1\ 0\ 0\ 0)_2$

$c_{3,j}=(1\ 1\ 1\ 0\ 0\ 1\ 0\ 1)_2$

where there is no case of all 1's or all 0's vertically, which is represented by Equations (E2) above. Hence the average Hamming weight is larger than zero (0) and smaller than one (1). If there is all 1's or all 0's vertically, the values do not satisfy Equation: $(c_{0,j} \text{ XOR } c_{1,j}) \lor (c_{1,j} \text{ XOR } c_{2,j}) \lor (c_{3,j} \text{ XOR } c_{3,j}) = (11111111)_2$, as shown on the following page:

$$\begin{array}{c} \text{all '1'} \qquad \text{all '0'} \\ c_{0,j}=(\,1\;1\;0\;1\;0\;0\;0\,)_2 \\ c_{1,j}=(\,0\;1\;0\;1\;0\;0\;1\;0\,)_2 \\ c_{2,j}=(\,1\;1\;0\;0\;1\;1\;1\;0\,)_2 \\ c_{3,j}=(\,0\;1\;1\;0\;1\;0\;1\;0\,)_2 \end{array}$$

$$c_{0,j}=(\,1\;1\;1\;0\;1\;0\;0\;0\,)_2$$
$$c_{1,j}=(\,0\;1\;0\;1\;0\;0\;1\;0\,)_2$$
$$c_{0,j}\oplus c_{1,j}=(\,1\;0\;1\;1\;1\;0\;1\;0\,)_2$$

$$c_{1,j}=(\,0\;1\;0\;1\;0\;0\;1\;0\,)_2$$
$$c_{2,j}=(\,1\;1\;0\;0\;1\;1\;1\;0\,)_2$$
$$c_{1,j}\oplus c_{2,j}=(\,1\;0\;1\;1\;1\;1\;1\;0\,)_2$$

$$c_{2,j}=(\,1\;1\;0\;0\;1\;1\;1\;0\,)_2$$
$$c_{3,j}=(\,0\;1\;1\;0\;1\;0\;1\;0\,)_2$$
$$c_{2,j}\oplus c_{3,j}=(\,1\;0\;1\;0\;0\;1\;0\;0\,)_2$$

$$\begin{array}{rl} & c_{0,j}\oplus c_{1,j}=(\,1\;0\;1\;1\;1\;0\;1\;0\,)_2 \\ \vee & c_{1,j}\oplus c_{2,j}=(\,1\;0\;1\;1\;1\;1\;1\;0\,)_2 \\ \vee & c_{2,j}\oplus c_{3,j}=(\,1\;0\;1\;0\;0\;1\;0\;0\,)_2 \\ \hline & \qquad\quad (\,1\;0\;1\;1\;1\;1\;1\;0\,)_2 \end{array}$$

20

The third clause of claim 8, in particular, recites:

q sets of fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equation, $FM_{0,h} = C_h \, XOR \, L1_0 \, (FMin_h)$, and $C_h = c_{h,15}c_{h,14}...c_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed mask values, where $Fmin_h$ is a selected one of said fixed mask values, and where i is an integer.

Kawamura neither teaches, discloses, nor suggests "q sets of fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equation, $FM_{0,h} = C_h \, XOR \, L1_0 \, (FMin_h)$, and $C_h = c_{h,15}c_{h,14}...c_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed mask values, where $Fmin_h$ is a selected one of said fixed mask values, and where i is an integer," as recited in claim 8. Both a positive integer not less than one and a plurality include two, and thus neither a positive integer not less than one nor a plurality anticipates "three or more," contrary to the assertion in the Office Action.

In addition, Kawamura does not mention equations $FM_{i,h} = C_h \, XOR \, L1_i(L2_{i-1}(D_h))$ for $i \geq 1$, $C_h = c_{h,15}c_{h,14}...c_{h,0}$, and $D_h = d_{h,15}d_{h,14}...d_{h,0}$ at all in paragraphs [0033]-[0037] or [0045]-[0052], contrary to the assertion in the Office Action in section 19 at page 7.

The fifth clause of claim 8 recites,

linear transform means $L1_i(x)$ and linear transform means $L2_i(x)$, wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed S-box table $S_{j,h} \, [x]$ and the linear transform means $L2_i(x)$ operate in i-th one of rounds.

Kawamura neither teaches, discloses, nor suggests "linear transform means $L1_i(x)$ and linear transform means $L2_i(x)$, wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed S-box table $S_{j,h} \, [x]$ and the linear transform means $L2_i(x)$ operate in i-th one of rounds," as recited in claim 8. Kawamura mentions no nonlinear transform at all, contrary to the assertion in the final Office Action in section 19 at page 7. DES, in fact, is described in the context of linear decryption at paragraphs [0004] and [0005]:

The DES has been evaluated in various viewpoints, and decryption methods such as a differential decryption method and linear decryption method, which are more effective than a key exhaustive search method, have been proposed. Note that the differential decryption method is disclosed in E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Journal of CRYPTOLOGY, Vol. 4, Number 1, 1991. The linear decryption method is disclosed in Mitsuru Matsui, "Linear Decryption of DES ciphertext (I)", Encryption and Information Security Symposium, SCIS93-3C, 1993.

Claim 8 is submitted to be allowable. Withdrawal of the rejection of claim 8 is earnestly solicited.

Claims 35, 36, and 37 depend from claim 8 and add additional distinguishing elements. Claims 35, 36, and 37 are thus also submitted to be allowable. Withdrawal of the rejection of claims 35, 36, and 37 is earnestly solicited.

Claims 38-41:

The third clause of claim 38 recites,

q sets of fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equations, $FM_{i,h} = C_h$ XOR $L1i(L2i\text{-}1(D_h))$ for $i \geq 1$, $C_h = c_{h,15}c_{h,14}...c_{h,0}$, and $D_h = d_{h,15}d_{h,14}...d_{h,0}$, are satisfied, where i is an integer.

Kawamura neither teaches, discloses, nor suggests "q sets of fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equations, $FM_{i,h} = C_h$ XOR $L1i(L2i\text{-}1(D_h))$ for $i \geq 1$, $C_h = c_{h,15}c_{h,14}...c_{h,0}$, and $D_h = d_{h,15}d_{h,14}...d_{h,0}$, are satisfied, where i is an integer," as discussed above with respect to the rejection of claim 8.

The fifth clause of claim 38 recites,

linear transform means $L1_i(x)$ and linear transform means $L2_i(x)$, wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed S-box table $S_{j,h}[x]$ and the linear transform means $L2_i(x)$ operate in i-th one of rounds.

Kawamura neither teaches, discloses, nor suggests "linear transform means $L1_i(x)$ and linear transform means $L2_i(x)$, wherein the linear transform means $L1_i(x)$, the nonlinear transform means with the masked fixed S-box table $S_{j,h}[x]$ and the linear transform means $L2_i(x)$ operate in i-th one of rounds," as discussed above with respect to the rejection of claim 8. Claim 38 is submitted to be allowable, for at least those reasons discussed above with respect to the rejection of claim 8. Withdrawal of the rejection of claim 38 is earnestly solicited.

Claims 39, 40, and 41 depend from claim 38 and add additional distinguishing elements. Claims 39, 40, and 41 are thus also submitted to be allowable. Withdrawal of the rejection of claims 39, 40, and 41 is earnestly solicited.

Claims 50-53:

The third clause of claim 50 recites,

q sets of masked fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equation, $FM_{0,h} = C_h$ XOR $L1_0(FMin_h)$, and $C_h = c_{h,15}c_{h,14}...c_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed mask values, where $FMin_h$ is a selected one of said fixed mask values, and where i is an integer.

Kawamura neither teaches, discloses, nor suggests "q sets of masked fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equation, $FM_{0,h} = C_h \, XOR \, L1_0 \, (FM_{i,h})$ and $C_h = c_{h,15}c_{h,1}...c_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed mask values, where i is an integer," as discussed above with respect to the rejection of claim 8.

The sixth clause of claim 50 recites,

said nonlinear transform means nonlinearly transforming an input thereto in accordance with said selected set of fixed S-box tables.

Kawamura neither teaches, discloses, nor suggests "said nonlinear transform means nonlinearly transforming an input thereto in accordance with said selected set of fixed S-box tables," as discussed above with respect to the rejection of claim 8. Claim 50 is submitted to be allowable, for at least those reasons discussed above with respect to the rejection of claim 8. Withdrawal of the rejection of claim 50 is earnestly solicited.

Claims 51, 52, and 53 depend from claim 50 and add additional distinguishing elements. Claims 51, 52, and 53 are thus also submitted to be allowable. Withdrawal of the rejection of claims 51, 52, and 53 is earnestly solicited.

Claims 54-57:

The third clause of claim 54 recites,

q sets of masked fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equations, $FM_{i,h} = C_h \, XOR \, L2_i(L1_{i-1}(D_h))$ for i≥1, $C_h = c_{h,15}c_{h,14}...c_{h,0}$, and $D_h = d_{h,15}d_{h,14}...d_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed mask values, where i is an integer.

Kawamura neither teaches, discloses, nor suggests "q sets of masked fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equations, $FM_{i,h} = C_h \, XOR \, L2_i(L1_{i-1}(D_h))$ for i≥1, $C_h = c_{h,15}c_{h,14}...c_{h,0}$, and $D_h = d_{h,15}d_{h,14}...d_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed mask values, where i is an integer," as discussed above with respect to the rejection of claim 8.

The sixth clause of claim 54 recites,

said nonlinear transform means nonlinearly transforming an input thereto in accordance with said selected set of fixed S-box tables.

Kawamura neither teaches, discloses, nor suggests "said nonlinear transform means nonlinearly transforming an input thereto in accordance with said selected set of fixed S-box tables," as

discussed above with respect to the rejection of claim 8. Claim 54 is submitted to be allowable, for at least those reasons discussed above with respect to the rejection of claim 8. Withdrawal of the rejection of claim 54 is earnestly solicited.

Claims 55, 56, and 57 depend from claim 54 and add additional distinguishing elements. Claims 55, 56, and 57 are thus also submitted to be allowable. Withdrawal of the rejection of claims 55, 56, and 57 is earnestly solicited.

Claims 64-67:

The fifth clause of claim 64 recites,

q sets of fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equations, $FM_{0,h} = C_h$ XOR $L1_0$ (FMin$_h$), and $C_h = c_{h,15}c_{h,14}...c_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed mask values, where $FMin_h$ is a selected one of said fixed mask values.

Kawamura neither teaches, discloses, nor suggests "q sets of fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equations, $FM_{0,h} = C_h$ XOR $L1_0$ (FMin$_h$), and $C_h = c_{h,15}c_{h,14}...c_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed mask values, where $FMin_h$ is a selected one of said fixed mask values," as discussed above with respect to the rejection of claim 8.

The tenth clause of claim 64 recites,

a plurality of nonlinear transform means for nonlinearly transforming an input in accordance with a fixed S-box table.

Kawamura neither teaches, discloses, nor suggests "a plurality of nonlinear transform means for nonlinearly transforming an input in accordance with a fixed S-box table," as discussed above with respect to the rejection of claim 8. Claim 64 is submitted to be allowable, for at least those reasons discussed above with respect to the rejection of claim 8. Withdrawal of the rejection of claim 64 is earnestly solicited.

Claims 65, 66, and 67 depend from claim 64 and add additional distinguishing elements. Claims 65, 66, and 67 are thus also submitted to be allowable. Withdrawal of the rejection of claims 65, 66, and 67 is earnestly solicited.

Claims 68-71:

The fifth clause of claim 68 recites,

q sets of fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equations $FM_{i,h} = C_h$ XOR $L1i(L2i-1(D_h))$ for i≥1, $C_h = c_{h,15}c_{h,14}...c_{h,0}$, and

$D_h = d_{h,15}d_{h,14}...d_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed mask values.

Kawamura neither teaches, discloses, nor suggests "q sets of fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, wherein equations $FM_{i,h} = C_h$ XOR L1i(L2i-1(D_h)) for i≥1, $C_h = c_{h,15}c_{h,14}...c_{h,0}$, and $D_h = d_{h,15}d_{h,14}...d_{h,0}$, are satisfied, where $FM_{i,h}$ is the i-th fixed value of the h-th set of said q sets of fixed mask values," as discussed above with respect to the rejection of claim 8.

The tenth clause of claim 68 recites,

a plurality of nonlinear transform means for nonlinearly transforming an input in accordance with a fixed S-box table.

Kawamura neither teaches, discloses, nor suggests "a plurality of nonlinear transform means for nonlinearly transforming an input in accordance with a fixed S-box table," as discussed above with respect to the rejection of claim 8. Claim 68 is submitted to be allowable, for at least those reasons discussed above with respect to the rejection of claim 8. Withdrawal of the rejection of claim 68 is earnestly solicited.

Claims 65, 66, and 67 depend from claim 68 and add additional distinguishing elements. Claims 65, 66, and 67 are thus also submitted to be allowable. Withdrawal of the rejection of claims 65, 66, and 67 is earnestly solicited.

Claim 72:

The second clause of claim 72 recites,

selecting one set of q sets of fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, in response to a random number h, where h is an integer between zero and q-1.

Kawamura neither teaches, discloses, nor suggests "selecting one set of q sets of fixed mask values $FM_{i,h}$, where q is an integer equal to three or more, in response to a random number h, where h is an integer between zero and q-1," as discussed above with respect to the rejection of claim 8.

The fifth clause of claim 72 recites,

nonlinearly transforming an input value in accordance with said selected set $S_{j,h}$ [x] of fixed S-box tables in that round.

Kawamura neither teaches, discloses, nor suggests "nonlinearly transforming an input value in accordance with said selected set $S_{j,h}$ [x] of fixed S-box tables in that round," as

discussed above with respect to the rejection of claim 8. Claim 72 is submitted to be allowable, for at least those reasons discussed above with respect to the rejection of claim 8. Withdrawal of the rejection of claim 72 is earnestly solicited.
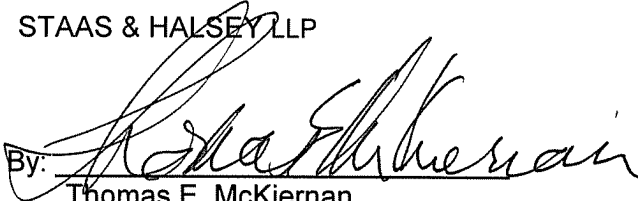
Conclusion:

Accordingly, in view of the reasons given above, it is submitted that all of claims 8, 35-41, 50-57, and 64-72 are allowable over the cited references. Allowance of all claims 8, 35-41, 50-57, and 64-72 and of this entire application is therefore respectfully requested.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: _17/1/07_

By: _____
Thomas E. McKiernan
Registration No. 37,889

1201 New York Avenue, NW, 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

Attachment: Clean Copy of Abstract